Encryption of E-mail

HIPAA Security◆May 2005

TMA Privacy Office Information Paper

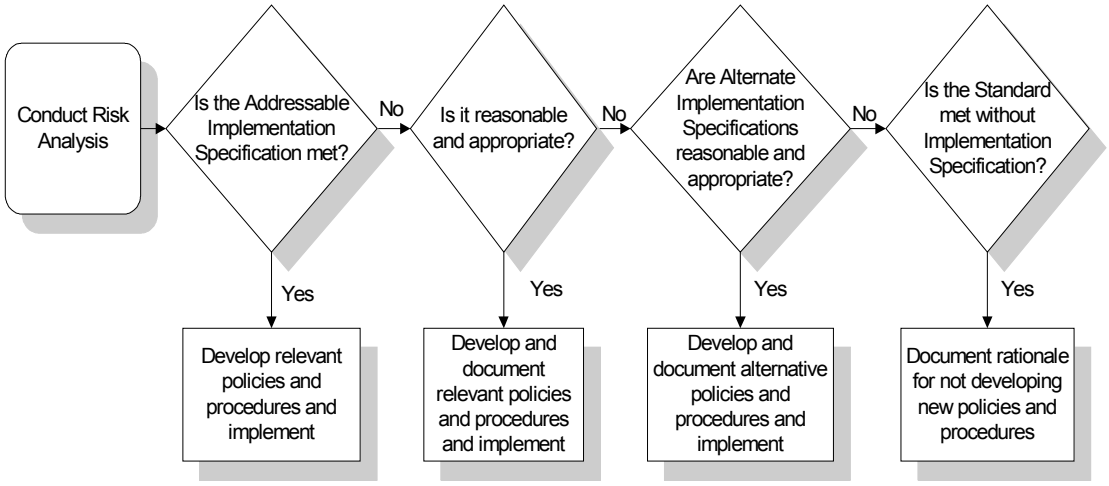
Records Management◆FOIA◆DUAs◆HIPAA Compliance◆ADP Security◆Privacy Act◆System of Records◆PIAs

General Requirement

The encryption implementation specification under the transmission security standard in the HIPAA Security Rule is addressable. It will remain addressable in the DoD regulation implementing that rule. Within HIPAA the term addressable has a very specific meaning that requires specific action on the part of the covered entity during their implementation efforts. The covered entity must carry out the implementation specification if it is reasonable and appropriate.

Process

The process for deciding what is reasonable and appropriate and documenting that is shown in the flow chart below.



This means that a password protected/encrypted zip file is one option for complying with the implementation specification, but not the only one. Which of the many methods available for protecting ePHI during transmission is implemented will depend on the outcome of the process depicted above. Factors to consider when determining if the implementation specification or alternate safeguard are reasonable and appropriate, include the degree of risk as determined through the risk assessment, cost of implementing the safeguard, capabilities of the hardware, software and technical infrastructure, your business processes, other safeguards already in place, and the size, complexity, and capabilities of the covered entity. The most important thing to keep in mind is to document the process used in determining what is reasonable and appropriate, especially the justification for using an alternate safeguard. Keep that as

Encryption of E-mail

part of your HIPAA documentation so it is available for IG and other types of inspections and in case there is ever an investigation as the result of a security incident or complaint.

Other Considerations

Another thing to keep in mind is that HIPAA does not specify what type or strength of encryption should be used. Therefore, if the risk management process determines that Microsoft encryption is the most reasonable and appropriate safeguard to use, then it is HIPAA compliant. While it may be HIPAA Compliant, you are also subject to other DoD regulation that specifies that when encrypting you must use encryption that has been certified for DoD use by either National Institute of Standards and Technology or the National Security Agency depending on the confidentiality level of the data being encrypted. DoD regulation (not HIPAA) also requires encryption for any "sensitive" data transmitted over a public network (not the Non-secure Internet Protocol Router Network).

Conclusion

The HIPAA Security Rule sets standards that implement a minimum level of protection. Every covered entity may implement safeguards that are stronger than those specified in the rule, just as each Service may levy requirements that are stronger than those promulgated by DoD. You should check to see what the requirements and restrictions are for transmission of PHI over networks in any Service level regulations to which you are subject. The TMA Privacy Office suggest that you work with each of the Services to determine what method of transmitting the ePHI will be most reasonable and appropriate and still comply with each of their differing transmission policies.